**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

Тема: «Разработка автоматизированного рабочего места преподавателя–ВВУЗ МО»

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Оглавление**

[**Введение** 3](#_Toc40087346)

[**Глава 1.** 6](#_Toc40087347)

[**1.1 Анализ современного состояния систем защиты информации от несанкционированного доступа** 6](#_Toc40087348)

[**1.2 Исследование возможностей проектирования и моделирования систем защиты информации от несанкционированного доступа в системе Министерства внутренних дел России** 13](#_Toc40087349)

[**Глава 2.** 21](#_Toc40087350)

[**2.1 Инструменты CPN Tools для создания имитационной модели системы защиты информации от несанкционированного доступа** 21](#_Toc40087351)

[**2.2 Имитационная модель системы защиты информации от несанкционированного доступа** 26](#_Toc40087352)

[**Глава 3. Сбор статистической информации** 36](#_Toc40087353)

[**3.1 Анализ полученной сети Петри** 36](#_Toc40087354)

[**3.2 Обоснование количества проходов по имитационной модели для получения адекватных характеристик модели системы защиты информации от несанкционированного доступа** 39](#_Toc40087355)

[**3.3 Анализ пространства состояний** 46](#_Toc40087356)

[**СПИСОК ЛИТЕРАТУРЫ** 52](#_Toc40087357)

**Введение**

Современный этап жизнедеятельности человека характеризуется глубокой информатизацией, которая связана с разработкой, эксплуатацией АС различного назначения. В связи с этим злоумышленниками постоянно совершенствуются способы получения конфиденциальной информации. Для предотвращения попыток НСД в АС внедряются СЗИ от НСД. Зачастую штатные пользователи таких систем пренебрегают своими должностными полномочиями и нарушают правила работы с защищенными системами. Пользовательские ошибки являются самыми распространенными, поэтому в работе мы допускаем, что была допущена ошибка и вредоносная программа проникла в АС. Будем считать, что нарушитель является внутренним с высоким потенциалом. Рассмотрим именно этот случай для съемного носителя информации CD/DVD/HD/Flesh.

Вредоносная программа может быть реализована в виде отдельного программного продукта (ПП) с функцией автозапуска при подключении к персональному компьютеру (ПК) в случае, когда пользователь сам отключает антивирусное программное обеспечение (ПО), т.к. зачастую АС потребляют большое количество ресурсов и, следовательно, работать становится неудобно, а зачастую невозможно из-за сильной загруженности.

Данные аспекты необходимо учитывать при разработке и эксплуатации СЗИ от НСД для определения ее вероятностно-временных характеристик в виде времен выполнения защитных функций, которые в дальнейшем планируется использовать при оценке эффективности ее функционирования, для установки взаимосвязей ее подсистем и компонентов, а также построения её логичной структуры в целом. Данная задача может быть решена при помощи построения имитационной модели СЗИ от НСД, которая и будет предопределять вышеперечисленные характеристики.

В качестве программной среды построения имитационной моделей в данной научной работе используем программу, разработанную в университете Орхуса (Дания) – CPN Tools. Отличительной особенностью CPN Tools является наличие обширного инструментария, позволяющего анализировать различные аспекты функционирования моделей на базе сетей Петри (безопасность и ограниченность позиций, уровень активности переходов, наличие тупиковых маркировок). CPN Tools используется во множестве реальных проектов в области телекоммуникации, при моделировании сетей и сетевых устройств, а также при верификации протоколов связи. В данной среде для построения моделей используются иерархические, временные, раскрашенные сети Петри, которые представляют собой универсальную алгоритмическую систему.

Система CPN Tools поддерживает язык Meta language (ML), который используется для описания операций, условий и функций. Благодаря применению ML программа позволяет упростить процесс построения и анализа моделей. В данный момент язык ML представляет большие перспективы, что в свою очередь обусловлено простотой языка как в изучении, так и в синтаксисе самого языка. Во многих институтах и университетах язык ML является одним из первых, для изучения, языков программирования наравне с C++, C#, JavaScript, PHP, Python. Это обусловлено тем, что большинство программных комплексов предназначенных для построений моделей сетевых и иных систем, описывающих работу программных средств и самой операционной системы, используют язык ML для инициализации математических функций. Имитационное моделирование в CPN Tools является дискретно-событийным, что предполагает мгновенную смену состояния сети Петри в определенные моменты времени, называемые шагами. Наличие временных меток позволяет моделировать процессы с учетом времени выполнения. Так же CPN Tools предоставляет различного вида отчёты, которые позволяют проанализировать построенную систему и сделать соответствующие выводы о системе в зависимости от целей исследования. Интерфейс программы CPN Tools является интуитивно понятным и достаточно прост в изучении, так же он предусматривает проверку работоспособности модели и выявление различных ошибок как в синтаксисе встроенного языка ML, так и в маркировке сети, что заметно облегчает работу с данной программой. Вывод оповещения об ошибке происходит в всплывающем «пузырьке» слева внизу, который имеет различные цвета. Желтый­ – означает процесс построения модели (ожидание), красный – указывает на ошибки различного рода, зеленый – выполнено успешно. Для получения подробной информации о происходящих процессах в ходе моделирования при наведении курсора мыши на «пузырек» отображается сообщение о процессе валидации модели.

## **Глава 1.**

## **1.1 Анализ современного состояния систем защиты информации от несанкционированного доступа**

Современная тенденция развития разных сфер человеческой деятельности характеризуется высоким уровнем информатизации. Особое внимание уделяется объектам, на которых обрабатывается конфиденциальная информация. К таким объектам можно отнести АИС различных государственных структур, включая ОВД, а также коммерческих организаций. Такие системы выполняют большое количество сложных задач, связанных с обработкой, хранением и передачей конфиденциальной информации.

Как показывает опыт эксплуатации АИС ОВД, на первый план в них выходят задачи, связанные с обеспечением надежности их функционирования и поддержанием на должном уровне ИБ этих систем. Существующая реальность показала, что максимальный вклад в нарушение ИБ АИС ОВД вносят факты, связанные с реализацией угроз несанкционированного доступа (НСД) к информационному ресурсу этих систем. Для защиты информации (ЗИ) от угроз НСД в АИС ОВД используются системы защиты информации (СЗИ от НСД), которые представляют собой сложные организационно-программные системы, являющиеся подсистемой ИБ в существующих АИС ОВД [16, 18]. Целью создания СЗИ от НСД в АИС ОВД является обеспечение ЗИ от незаконного доступа к информационному ресурсу, уничтожения, модификации, блокирования, копирования информации и иных действий, ведущих к нарушению функционирования АИС ОВД [17].

При создании информационных систем для автоматизации оперативно-служебной деятельности подразделений ОВД необходимо использовать единые требования и методику систем автоматизированного проектирования (САПР) СЗИ от НСД [16], создание которой позволит значительно повысить надежность разрабатываемых СЗИ от НСД и защищенность АИС, что позволит учитывать особенности их функционирования, например, такие как ресурсоемкость, количество затрачиваемого процессорного времени АИС, оперативной памяти и т.д. на их функционирование, что приводит к значительному увеличению времени отклика АИС на запросы и, как следствие, к уменьшению эффективности ее работы (снижение «оперативности»). Сегодня СЗИ от НСД в период эксплуатации выполняют множество задач, связанных с мониторингом АИС, поэтому необходимо учитывать влияние их функционирования на работу АИС ОВД по прямому назначению (обработка, хранение и передача конфиденциальной информации), связанных со значительным отвлечением вычислительных ресурсов АИС ОВД, что отрицательно влияет на работоспособность системы в целом. Таким образом, методика выбора оптимальных СЗИ от НСД в АИС ОВД требует тщательной разработки с учетом вышеуказанных особенностей функционирования этих систем. На практике выбор СЗИ от НСД в АИС ОВД происходит следующим образом. Администратор получает категорированный компьютер, либо собирает его на основании соответствующего разрешения. Вводит в эксплуатацию на объекте информатизации ОВД СЗИ от НСД. По мере появления задач, связанных с разграничением доступа пользователей, меняется политика защиты администратором и, соответственно, характеристики СЗИ от НСД. Изменения в конфигурации СЗИ от НСД влекут за собой появление новых уязвимых мест, что ведет к повышению влияния уровня угроз НСД, связанных с утечкой конфиденциальной информации. Такой подход является во многом необоснованным и непрофессиональным, это связано с непониманием принципов работы всех ключевых частей системы. По причине отсутствия цельной методики САПР СЗИ от НСД в АИС ОВД администратор и даже штат сотрудников отделов информационных технологий не в силах сами разработать эти системы. Комплексный и научный подход к проблеме ЗИ в АИС ОВД способен решить вышестоящие задачи. Актуальность создания СЗИ от НСД подтверждена приказом МВД России от 14.03.2012 № 169, который нацелен на совершенствование систем ИБ в ОВД. В нем прописаны цели, задачи, принципы, основные направления обеспечения ИБ, одним из механизмов решения которых является разработка критериев и методов оценки эффективности систем обеспечения ИБ ОВД, однако методика проектирования СЗИ от НСД (включающая математическое, алгоритмическое обеспечение создания этих систем) в данном приказе не приведена.

Существующие СЗИ от НСД содержат в своем составе комплекс программных средств защиты от НСД в АИС ОВД [16]. В данной статье в качестве типового объекта защиты рассматривается локальная сеть (вычислительная система), которая является элементом большой распределенной АИС ОВД. Таким образом, как объект разработки СЗИ от НСД представляет собой сложную систему, включающую различные программно-технические и программно-методические комплексы, характеризующиеся большим количеством разнородных параметров (количественных и качественных). Поэтому для разработки СЗИ от НСД в АИС ОВД необходимо создание соответствующего математического, алгоритмического и программного обеспечения (ПО) с целью разработки единой методики САПР СЗИ от НСД в ОВД, что и является направлением дальнейшего исследования.

В настоящее время планируется переход всех АРМ ОВД на ОС Astra Linux. Это позволит значительно улучшить защиту информации, поскольку комплекс средств защиты (КСЗ) обеспечивает следующие функции (Рисунок 1.1.):

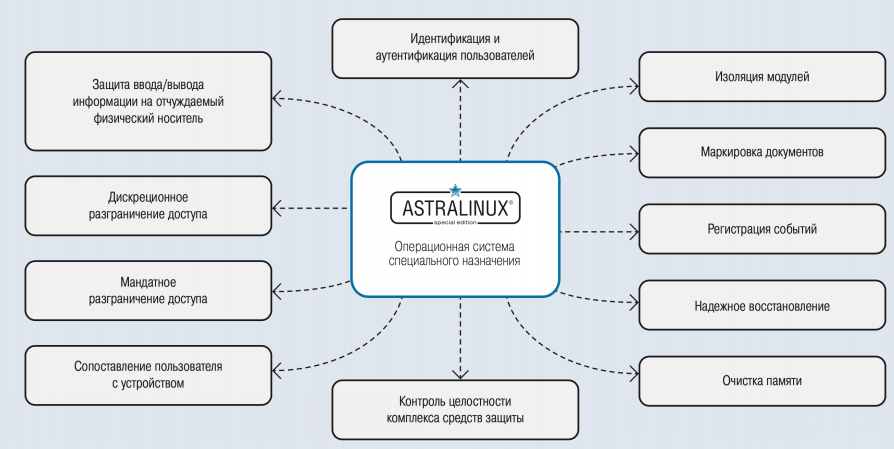


Рисунок 1.1. Комплекс средств защиты ОС Астра Linux

Реализация этих функций основана на следующих основных положениях:

1. с каждым пользователем системы связан уникальный численный идентификатор — идентификатор пользователя (UID), который является ключом к соответствующей записи в БД пользователей, содержащей информацию о пользователях, включая их реальные и системные имена. БД пользователей поддерживается и управляется системным администратором. UID является ярлыком субъекта (номинальный субъект), которым система пользуется для определения прав доступа. БД пользователей в ОС может быть как локальной для системы, так и являться частью единого пространства пользователей, функционирующего на основе протокола LDAP, использующий TCP/IP и позволяющий производить операции аутентификации;
2. каждый пользователь входит в одну или более групп. Группа — это список пользователей системы, имеющий собственный идентификатор (GID). Поскольку группа объединяет несколько пользователей системы, в терминах политики безопасности она соответствует понятию «множественный субъект». GID является ярлыком множественного субъекта, которых у номинального субъекта может быть более одного. Таким образом, одному UID соответствует список GID;
3. роль действительного (работающего с объектами) субъекта играет процесс. Каждому процессу присваивается единственный UID, являющийся идентификатором запустившего процесс номинального субъекта, т. е. пользователя. Процесс, порожденный некоторым процессом пользователя, наследует UID родительского процесса. Таким образом, все процессы, запускаемые пользователем, имеют его идентификатор. Все процессы, принадлежащие пользователю, образуют сеанс пользователя. Первый процесс сеанса пользователя порождается после прохождения процедур идентификации и аутентификации. При обращении процесса к объекту доступ предоставляется по результатам процедуры авторизации, т. е. обработки запроса на основе мандатных и дискреционных прав доступа;
4. механизм распределения доступа реализован в ядре ОС, что обеспечивает его правильное функционирование при использовании любых компонентов, предоставляемых ОС. Реализация мандатного управление доступом затрагивает все подсистемы ядра, в которых реализовано дискреционное управление доступом. При этом оба вида управления доступом функционируют параллельно, не влияя на принятие решений друг друга (непротиворечивость). Доступ разрешается в том случае, если он возможен относительно дискреционных и мандатных прав доступа. Запрещается в случае, если доступ запрещен относительно любого из механизмов.

В ОС Windows базовые средства защиты информации не обеспечивают надежного хранения и предотвращения доступа к информации. Для того чтобы это исправить используются сторонние СЗИ от НСД такие как Страж NT, DALLAS LOCK, Secret Net, ПАК «Соболь», КСЗИ «Панцирь+». Например, Страж NT обеспечивает следующие функции:

* Двухфакторная аутентификация до загрузки операционной системы (в том числе и для виртуальной среды) с использованием аппаратных идентификаторов:
* USB-идентификаторов типа Guardant ID, Рутокен, eToken, JaCarta, ESMART Token;
* смарт-карт Рутокен, eToken, JaCarta, ESMART;
* iButton;
* Дискреционный принцип контроля доступа к ресурсам системы.
* Мандатный принцип контроля доступа к ресурсам системы, в том числе:
* возможность одновременной работы с документами разных грифов в одном сеансе (без смены сеанса пользователя);
* контроль именованных каналов.
* Создание замкнутой программной среды пользователя, позволяющей ему запуск только разрешенных приложений.
* Регистрация событий безопасности, в том числе и действий администратора.
* Маркировка выдаваемых на печать документов независимо от печатающего их приложения.
* Гарантированная очистка:
* освобождаемой оперативной памяти;
* содержимого защищаемых файлов при их удалении;
* файла(ов) подкачки при завершении работы системы.
* Контроль целостности защищаемых ресурсов системы и компонентов системы защиты информации.
* Управление пользователями.
* Управление носителями информации.
* Управление устройствами.
* Преобразование информации на отчуждаемых носителях.
* Тестирование системы защиты информации.

Таким образом можно сделать вывод, что концептуальные подходы к ЗИ в ОС ОВД не поменялись. Значительным преимуществом в пользу ОС Астра Linux является, то что все подсистемы ЗИ встроены в саму ОС, а не устанавливаются отдельно. Приложения, используемые в ОС Астра Linux, перед установкой сравниваются путем проверки их контрольных сумм, следовательно, установить не проверенное приложение из неизвестного источника не получится. Также данная ОС является отечественной разработкой.

## **1.2 Исследование возможностей проектирования и моделирования систем защиты информации от несанкционированного доступа в системе Министерства внутренних дел России**

Объект проектирования СЗИ НСД представляют собой сложную организационно-техническую систему, включающую различные программно-технические (ПТК) и программно-методические комплексы (ПМК) и характеризующуюся большим количеством разнородных параметров. Поэтому создание СЗИ НСД требует разработки соответствующего математического обеспечения и ПО, предназначенного для построения и повышения эффективности систем автоматизированного проектирования (САПР). При этом следует учитывать, что большой объем задач может быть решен программными средствами ЗИ, которые являются важнейшей и непременной частью механизма защиты современных АС ОВД от НСД, что определяется следующими их достоинствами: универсальностью; надежностью; простотой реализации; возможностью модификации и развития.

Принцип параллельного проектирования СЗИ НСД совместно с разработкой самой защищаемой АС, начиная с формулировки общего замысла ее построения, и на всех основных этапах: разработка технического предложения; эскизный и технический проекты; выпуск рабочей документации; испытания и сдача заказчику. Невыполнение этого принципа может привести к низкой эффективности защиты, отвлечению дополнительных ресурсов и увеличению затрат на обеспечение ИБ. Таким образом, требования к СЗИ НСД образуют иерархическую систему и должны включаться: в общее техническое задание на АС; в частные ТЗ на подсистемы, ПТК, технические средства; в ТЗ на организацию интерфейса с внешними системами; в ТЗ на базовое и прикладное ПО.

Другими принципами являются:

1. создание СЗИ НСД должно осуществляться разработчиками такого же уровня, что и самой АС;
2. привлечение к созданию СЗИ НСД специалистов широкого профиля, обеспечивающих комплексное решение вопросов ЗИ, разработки ПО и ПТК, организационных и системных;
3. простота СЗИ НСД, т.е. она должна с минимальной избыточностью удовлетворять требованиям по необходимой эффективности, что повышает ее надежность, экономичность, уменьшает влияние на временные характеристики АС;
4. удобство обращения с СЗИ НСД, "прозрачность" для пользователя АС.

Этапы разработки СЗИ НСД.

* + 1. Анализ информационно-технических характеристик АС и формирование множества исходных данных для разработки СЗИ НСД: определяется состав необходимых параметров АС, в зависимости от которых будет проектироваться СЗИ НСД.
    2. Анализ требований к ИБ в АС, формирование ТЗ на разработку СЗИ НСД: на данном этапе проводится полный анализ исходных данных, выработка требований к СЗИ НСД в АС, формирование набора показателей ее эффективности и установление их граничных значений, обеспечивающих минимально допустимый уровень ИБ (защиты) и составляется техническое задание на разработку СЗИ НСД.
    3. Выявление и анализ возможных каналов НСД: поиск всех возможных каналов утечки и НСД (через локальные, глобальные компьютерные сети и другие способы доступа, технические каналы и т.д.) анализ этих каналов для дальнейшего создания СЗИ НСД. Определение соответствующего перечня угроз информации, формирование содержательных и формализованных моделей информационных угроз.
    4. Формирование модели потенциальных нарушителей: на основе нормативной документации, литературных источников, предшествующего опыта и специфических условий работы АС проводится формирование модели потенциальных нарушителей, включающее выбор содержательной модели поведения потенциальных нарушителей, определение конкретного подмножества из всех выявленных каналов НСД в АС и утечки информации, потенциально возможных каналов для использования нарушителями определенного класса.
    5. Формирование требований для выбора или разработки технических и программных средств ЗИ: производится на основе анализа возможных каналов НСД, потенциальных угроз ИБ, нарушителей. Средства ЗИ должны обеспечивать перекрытие существующих и предупреждение появления новых каналов НСД и утечки.
    6. Выбор или разработка ПСрЗИ: выбор ПСрЗИ из уже существующих или, при необходимости создание новых СЗИ НСД, обеспечивающих более надежную защиту от НСД.
    7. Выбор технических средств ЗИ: они должны отвечать необходимым требованиям к СЗИ НСД, обеспечивая необходимую защиту на аппаратном уровне, соответствовать требованиям, предъявляемым со стороны ПСрЗИ, обеспечивать совместимость и стабильную работу программ ЗИ.
    8. Структурный синтез и оптимизация состава СЗИ НСД, обеспечивающей перекрытие всех каналов НСД и утечки с требуемым уровнем эффективности (вероятности защиты).
    9. Анализ и оценка критерия эффективности комплекса средств ЗИ (КСЗИ) (прочности защиты): оценка эффективности (прочности) каждого предлагаемого средства ЗИ относительно всех перекрываемых им каналов (нейтрализуемых угроз) утечки и НСД. Если выявлены недостатки СЗИ НСД, то вырабатываются методы устранения этих недостатков.
    10. Доработка (модификация, адаптация) и параметрическая оптимизация КСЗИ: устранение недостатков средств ЗИ, адаптация их к используемым СВТ и условиям функционирования.
    11. Комплексирование и оценка эффективности ПТК ЗИ (СЗИ НСД): интеграция подсистем и элементов СЗИ НСД в АС для обеспечения информационной совместимости, централизованного контроля и управления со стороны автоматизированных рабочих мест администраторов и служб ИБ; комплексная оценка эффективности всего программно-технического комплекса СЗИ НСД на предмет защиты от НСД и стабильности работы в критических ситуациях. В случае обнаружения недостатков системы проводится дополнительная доработка ее компонентов и их взаимодействия, замена отдельных средств защиты, введение дублирования для наиболее опасных угроз (каналов) и т.д.

В результате проведения рассмотренных процедур может быть получен высокоустойчивый к заданным внешним и внутренним воздействиям программно-технический комплекс ЗИ.

Анализ содержания этих этапов позволяет сделать вывод, что они содержат задачи как слабоформализуемые, требующие для выполнения квалифицированных специалистов, привлечения экспертов, применения эвристических методов и подходов, так и такие, которые могут быть формализованы в рамках задач и методов структурного синтеза, параметрической идентификации и оптимизации с привлечением положений теории математического программирования.

Стоит учитывать, что модель должна быть дискретно-событийной поскольку время задано точно, и этому времени соответствует какое-либо событие. Эти времена накладываются одно на другое и получается диаграмма событий во времени. Таким образом, рассчитываются только те события, которые проходят, и тем самым экономится время счета.

Исходя из этого, дискретно-событийное моделирование является весьма экономичным, так как программа считает только в точках измерения состояния модели, отвечает сути изучаемых процессов, главным из которых является последовательность событий, и обладает точным временем в отношении начала и завершения событий, так как времена рассчитываются без погрешностей.

Для создания модели СЗИ от НСД следует воспользоваться имитационным моделированием. Главное отличие от аналитических моделей – построение алгоритма (последовательности действий), который отображает процессы внутри исследуемого объекта, и воспроизводят его поведение на АРМ. Такие модели применяются тогда, когда описать модель поведения объекта математическими уравнениями невозможно или затруднительно. Данный подход позволяет отделять части от большой модели, которые, в свою очередь, тоже можно разделить на части.

Итак, основное преимущество имитационного моделирование в отличие от аналитического является возможность решения сложных задач, так как модель можно усложнять в процессе моделирования и результативность не упадет. Воспроизводя алгоритм работы системы во времени, и имитируются явления, составляющие процесс, сохраняющие логическую структуру и последовательность действия, что позволит получить сведения о состояниях процесса в определенные моменты времени, что позволяет получить характеристики системы и провести анализ. Имитационные модели позволяют достаточно просто учитывать такие факторы, как наличие дискретных и непрерывных элементов, многочисленные случайные воздействия, нелинейные характеристики элементов системы, которые создают трудности при аналитических исследованиях. Имитационное моделирование стремится к объектно-ориентированному представлению, которое естественным образом описывает объекты, их состояние, поведение и взаимодействие между ними.

Имитационная модель в отличие от аналитической представляет собой не законченную систему уравнений, а развернутую схему с детально описанной структурой и поведением изучаемого объекта. Для имитационного моделирования характерно воспроизведение явлений, описываемых моделью, с сохранением их логической структуры, последовательности чередования во времени, взаимосвязей между параметрами и переменными исследуемой системы. В аналитических моделях можно использовать широкий арсенал математических методов, что часто позволяет найти оптимальное решение и иногда провести анализ чувствительности. Чтобы получить оптимальное решение имитационной модели нужно провести множество испытаний этой модели. Но с помощью такого подхода можно получить такие данные, которые получить с помощью аналитических моделей трудно или невозможно, например, поведение модели до достижения устойчивого состояния.

В аналитических моделях значения переменных являются выходными данными модели, а результатом процесса оптимизации модели будут значения которые минимизируют или максимизируют целевую функцию. В имитационных моделях значения переменных будут входом модели, а выходным результатом – значение целевой функции, соответствующее входным значениям.

Аналитические модели трудны для формализации и построения, эти модели имеют факторы которые затрудняют построение в зависимости от специфики модели. Так же аналитические методы дают среднестатистические или стационарные решения, но на практике важно именно нестационарное поведение системы или ее характеристики на коротком временном интервале, что не позволяет получить усредненное значение.

Для имитационного моделирования можно использовать широкий набор ПО для создания этих моделей обеспечивая возможность измерения интересующих параметров модели и исследования сложных сценариев поведения системы.

В настоящее время существует большое разнообразие программных средств моделирования. Рассмотрим некоторые из них, наиболее распространенные в мире и имеющие широкие возможности функционирования. Параллельно также проведем сравнительный анализ таких программных средств моделирования, как: GPSS/H, GPSSWorld, Extend, CPN Tools.

Программный продукт GPSS/H (WolverineSoftware, США) предназначен для моделирования систем массового обслуживания и других систем, например, системы распределения ресурсов между потребителями. Благодаря блочной структуре GPSS/H может быть легко приспособлен для структурно-функционального моделирования не очень сложных систем. Это программное средство имеет функции, переменные, стандартные атрибуты, графики и статические блоки, что расширяет функциональные возможности пакета GPSS/H.

GPSSWorld – самая современная версия языка имитационного моделирования GPSS для персональных ЭВМ и OC Windows. Программное средство GPSSWorld обладает высочайшим уровнем интерактивности и визуального представления информации. GPSSWorld имеет анимационные возможности и является объектно-ориентированным языком, что позволяет наблюдать и фиксировать внутренние механизмы работы моделей. Интерактивность языка предоставляет возможность одновременного исследования и управления процессами моделирования. Возможно вычисление доверительных интервалов и дисперсионного анализа.

Программное средство моделирования Extend (ImagineThat, Inc., США) имеет мощный графический интерфейс (2D, 3D), позволяет создавать стохастические динамические модели любого предприятия. Extend обладает некоторыми недостатками по сравнению с другими программными средствами. Например, моделирование требует частичного написания кода при задании свойств блоков. К недостаткам можно отнести и то, что система Extend используется для моделирования процесса, который может быть представлен в виде «блок-схем».

CPN Tools – это специальная моделирующая система, которая использует язык сетей Петри для описания моделей. Система была разработана в Университете Орхуса в Дании и свободно распространяется для некоммерческих организаций через сайт <http://www.daimi.au.dk/CPNTools/>. Уровень предоставляемого сервиса позволяет классифицировать CPN Tools как промышленную моделирующую систему. Она была использована в большом количестве реальных проектов, особенно в области телекоммуникаций. В последнее время корпорация Nokia применяет CPN Tools для управляемой моделью разработки нового поколения мобильных телефонов. CPN Tools предлагает очень мощный класс сетей Петри для описания моделей. Согласно стандартной классификации такие сети называют иерархическими временными раскрашенными сетями Петри. Было доказано, что они эквивалентны машине Тьюринга и составляет универсальную алгоритмическую систему. Таким образом, произвольный объект может быть описан с помощью этого класса сетей.

Для решения задач, связанных с проектированием защищенных автоматизированных систем в ОВД лучше всего подходит программный продукт CPN Tools, поскольку он обладает рядом преимуществ перед другими средствами имитационного моделирования, такими как безопасность и ограниченность позиций, отображение уровня активности переходов, наличие тупиковых маркировок, обширность инструментария, позволяющего проанализировать как отдельную позицию, так и всю модель в целом.

# **Глава 2.**

## **2.1 Инструменты CPN Tools для создания имитационной модели системы защиты информации от несанкционированного доступа**

CPN Tools предлагает обширный инструментарий для создания моделей основанных на сетях Петри. Для построения модели СЗИ от НСД понадобятся следующие инструменты:

- палитра «Create» (рисунок 2.1), предназначена для создания вершин и дуг между ними, содержащая нужные элементы, такие как

* Creates a transition
* Creates a place
* Creates an arc

****

Рисунок 2.1.Палитра инструментов «Create»

- Палитра «Simulation» (Рисунок 2.2), содержит инструменты для запуска процесса моделирования и содержит такие элементы как

* Goes to the initial state
* Stop an ongoing simulation
* Executes a transition with a chosen binding
* Executes a transition
* Executes the specified number of transition



Рисунок 2.2. Панель инструментов «Simulation»

- Панель инструментов «State Space» (Рисунок 2.3), содержит в себе инструменты для расчета пространства состояний и построения SCC графа.

* Calculate State Space
* Calculate SCC graph
* Save report
* Display the node with the specified number

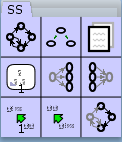


Рисунок 2.3. Панель инструментов «State Space»

- Панель инструментов «Style» (Рисунок 2.4) позволяет раскрасить нужные элементы модели в нужные цвета



Рисунок 2.3. Панель инструментов «Style»

- Панель инструментов «View» (Рисунок 2.4) позволяет изменять масштаб модели.



Рисунок 2.4. Панель инструментов «View»

Для создания надежных взаимосвязей между подсистемами СЗИ от НСД воспользуется палитрой инструментов «Hierarchy» (рисунок 2.5) в CPN Tools в состав которой входят инструменты:

* создать переход на подсеть;
* замена перехода на подсеть;
* назначить подсеть для перехода;
* назначить порт для перехода;
* установить тип порта IN;
* установить тип порта OUT;
* установить тип порта IN / OUT;
* разместить переход в одном месте.

Для реализации перехода между подсистемами СЗИ от НСД воспользуемся инструментом «Assigns subpage for a substitution transistion», а именно выбрать переход, который будет передавать маркер из одной подсистемы в другую. Например, переход между вершинами r29 и r39 (рисунок 2.6).

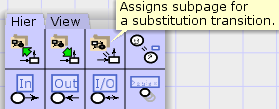


Рисунок 2.5. Меню панели инструментов «Hierarchy»

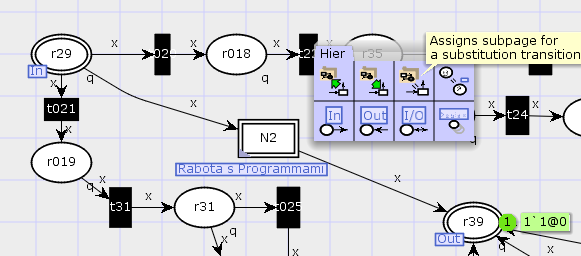


Рисунок 2.6. Инструмент «Assigns subpage for a substitution transistion»

На следующем этапе перейдем на последующую часть имитационной модели, которая будет являться выходной и воспользуемся инструментом «Sets the port type to In». Данный инструмент необходим для того, чтобы назначить входную вершину для передачи маркера из одной сети в другую. (рисунок 2.7).

Следующим шагом в построении иерархической имитационной модели используем инструмент «Sets the port type to Out» для того чтобы назначить выходную вершину дочерней сети (рисунок 2.8).

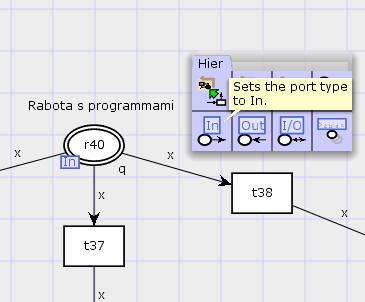


Рисунок 2.7. Инструмент «Sets the port type to In»

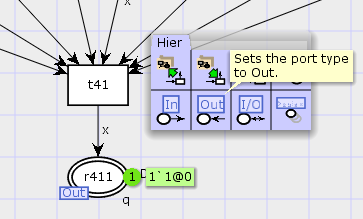


Рисунок 2.8. Инструмент «Sets the port type to Out»

Завершающий этап будет характеризоваться установкой связей между выходными вершинами родительской и дочерней сети при помощи инструмента «Assigns a port to a socket» (рисунок 2.9).

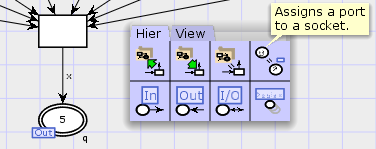


Рисунок 2.9. Инструмент «Assigns a port to a socket»

Так как связей между подсистемами достаточно много нельзя очевидно сказать, что какая то из подсистем является родительской, а какая то дочерней нельзя, поэтому построение имитационной модели следует начать с ее первой подсистемы.

Введем следующие обозначения для вершин и переходов. Вершины в нашей модели используются двух видов это вершины с индексами r1 и т.д. представляют собой функции, выполняемые СЗИ от НСД, а вершины с индексами r01 и т.д. являются дополнительными, требующимися для ввода вероятностей. И соответственно переходы с индексом t1 и т.д., являются основными, а t01 и т.д. являются дополнительными.

## **2.2 Имитационная модель системы защиты информации от несанкционированного доступа**

Моделирование СЗИ от НСД представляет собой сложный процесс. Первоначальным этапом разработки модели является построение ее подсистем и их компонентов, полностью идентичных реально функционирующей СЗИ от НСД с целью получения ее свойств и характеристик. В связи с этим наша модель будет состоять из следующих подсистем:

* Подсистема «Включение ПК и идентификации пользователя»;
* Подсистема «Инициализации прав пользователя на работу в системе и доступ к каталогу файлов»;
* Подсистема «Работа пользователя с файлами и программами»;
* Подсистема «Работа пользователя с прикладными программными продуктами»;
* Подсистема «Деструктивное воздействие на СЗИ от НСД».

Первая модель отображает вход пользователя в СЗИ от НСД посредством его аутентификации (рисунок 2.10). Данная модель даёт визуальное представление о том, что происходит в системе при входе пользователя. Из рисунка 2.10 видно, что при неправильном вводе пароля (после 3 раза) следует блокировка автоматизированного рабочего места, что позволяет обеспечить защиту персонального компьютера от брутфорса. Переход T01 обеспечивает передачу маркера в подсистему «Инициализации прав пользователя на работу в системе и доступ к каталогу файлов в системе» а также, что в позиции r12 реализован случай блокировки допуска к вводу пароля. В таблице 2.1 приведены состояния рассматриваемой подсистемы.

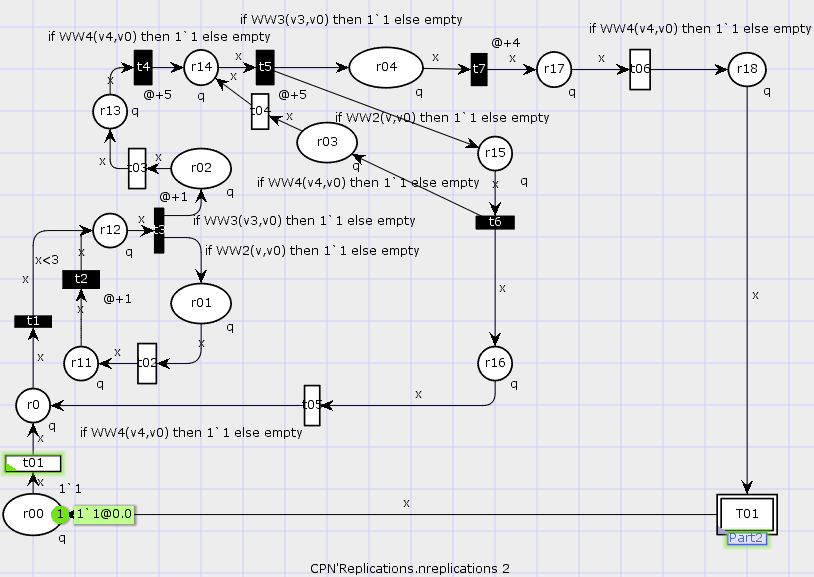


Рисунок 2.10. «Включение АРМ и идентификации пользователя»

Таблица 2.1. Подсистема «Включения АРМ и идентификации пользователя»

|  |
| --- |
| Функции, выполняемые СЗИ от НСД |
| 0 Включение АРМ  (Прекращение выполнения функций АРМ) |
| 1.1 Предъявление идентификатора |
| 1.2 Прекращение работы идентификатора |
| 1.3 Допуск к вводу пароля |
| 1.4 Ввод пароля |
| 1.5 Повторный ввод пароля |
| 1.6 Блокировка входа в систему при трехразовом неправильном вводе пароля |
| 1.7 Аутентификация субъекта системы |
| 1.8 Вход в систему |

Вторая модель отображает «Инициализацию прав пользователя на работу в системе и доступ к каталогу файлов» (Рисунок 2.11). В точке r241 реализуется вход из подсистемы «Деструктивного воздействия на СЗИ от НСД». После перехода пользователя к работе с носителем, вредоносная программа автоматически запускается и в имитационной модели появляется новый «маркер», который представляет собой деструктивное программное воздействие на СЗИ от НСД, которое направлено на получение доступа к информации. В таблице 2.2 приведены состояния рассматриваемой подсистемы.

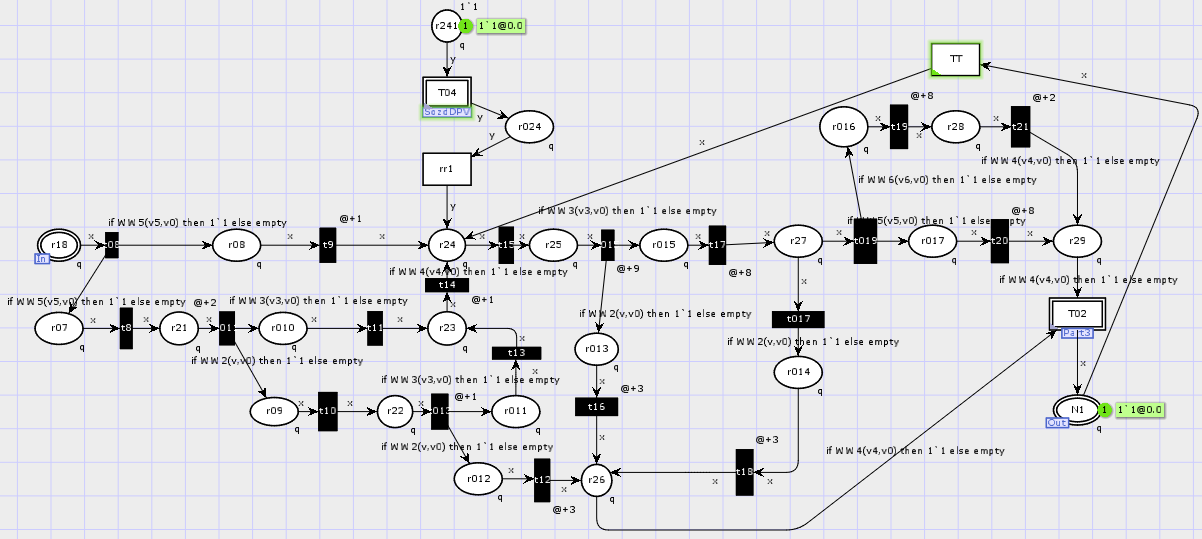


Рисунок 2.11. «Инициализацию прав пользователя на работу в системе и доступ к каталогу файлов»

Таблица 2.2. «Инициализацию прав пользователя на работу в системе и доступ к каталогу файлов»

| Функции, выполняемые СЗИ от НСД |
| --- |
| 1.8 Вход в систему |
| 2.1 Сопоставление идентификационной информации внешнего носителя и пользователя |
| 2.2 Контроль устройств (если устройство не принадлежит пользователю, срабатывает данный механизм) |
| 2.3 Доступ к внешнему носителю |
| 2.4 Обращение к объекту на носителе |
| 2.5 Сопоставление меток конфиденциальности пользователя и ресурса (в СЗИ реализуется на основе мандатного принципа контроля доступа) |
| 2.6 Блокировка доступа к объекту |
| 2.7 Проверка полномочий доступа пользователя (в СЗИ реализуется на основе дискреционного принципа контроля доступа) |
| 2.8 Преобразование информации на носителе при помощи шифрования (в СЗИ применяется метод гаммирования) |
| 2.9 Допуск субъекта к защищаемому объекту |

Следующая модель подсистемы описывает работу пользователя с отдельными объектами защищаемой системы (Рисунок 2.12), основанной на принципе разграничения доступа по аутентификации пользователя и ограничения его прав доступа к отдельным объектам системы.

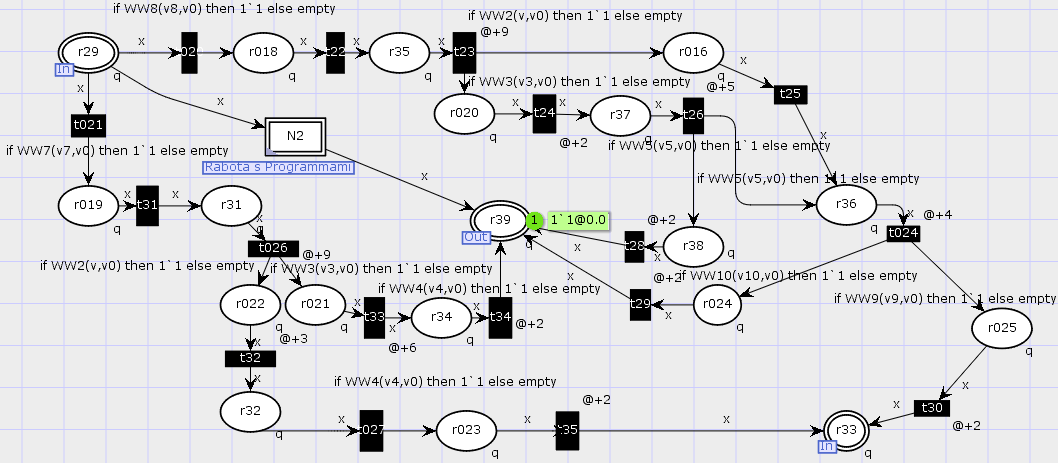


Рисунок 2.12. «Работа пользователя с файлами и программами»

В случае, если пользователю запрещено работать с отдельными объектами, то СЗИ от НСД блокирует доступ к объекту и записывает информацию о данном факте в журнале событий. Это помогает выявлять факты НСД пользователя к объектам, к которым он не имеет доступа. Данный функционал заложен во вредоносную программу для того, чтобы провести имитацию реакции СЗИ от НСД на действия злоумышленника. В вершине r29 реализован переход на подсистему «Работа пользователя с прикладными программными продуктами», которая моделирует работу пользователя с отдельными ПП.

Таблица 2.3. «Работа пользователя с файлами и программами»

|  |
| --- |
| Функции, выполняемые СЗИ от НСД |
| 2.9 Допуск субъекта к защищаемому объекту |
| 3.1 Запрос на преобразование объекта |
| 3.2 Блокировка преобразования объекта |
| 3.3 Регистрация нарушений работы с СЗИ |
| 3.4 Пересчет параметров целостности файла |
| 3.5 Запрос на удаление |
| 3.6 Блокировка удаления |
| 3.7 Преобразование объекта перед удалением |
| 3.8 Удаление объекта |
| 3.9 Завершение работы с объектом |

Модель подсистемы «Работа пользователя с прикладными программными продуктами» (рис. 2.13) включает в себя наиболее распространенное ПО. Данная подсистема взаимодействует с подсистемой «Работа пользователя с файлами и программами», соединительной вершиной между ними является r411. Необходимо отметить, что в модели мы рассматриваем работу только с одним ПП, без возможности использовать другие программы параллельно. Данная система отражает работу пользователя с типовым составом ПП, в частности с такими как Microsoft Office, ABBY Fine Reader, Nero, WinRar, Total Commarder.

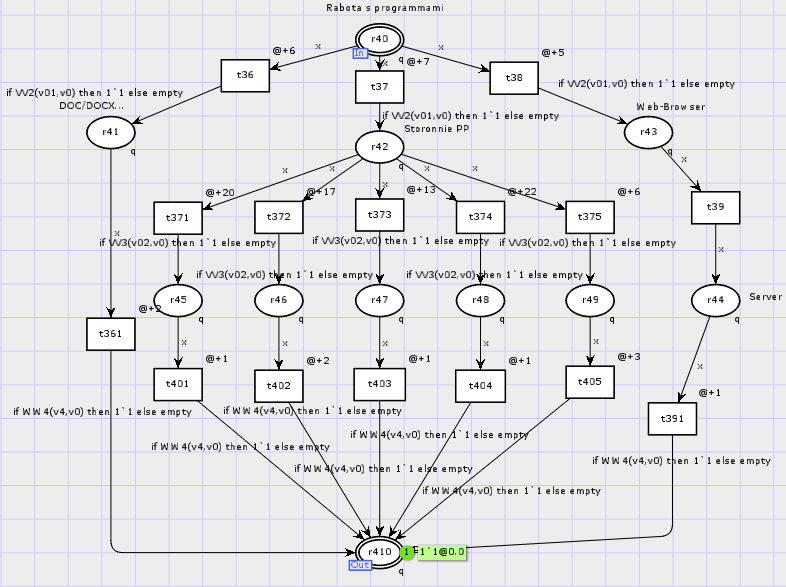


Рисунок 2.13. «Работа пользователя с файлами и программами»

Таблица 2.4. «Работа пользователя с файлами и программами»

|  |
| --- |
| Функции, выполняемые СЗИ от НСД |
| 4 Начало работы с программами |
| 4.1 Работа с документами |
| 4.2 Работа с отдельным ПО |
| 4.3 Работа с браузером и в сети(локальной/глобальной) |
| 4.4 Использование различных серверов в интернете |
| 4.5 Работа с ПП Microsoft Office |
| 4.6 Работа с ПП ABBY Fine Reader |
| 4.7 Работа с ПП Nero |
| 4.8 Работа с ПП WinRar |
| 4.9 Работа с ПП Total Commarder |
| 4.10 Полученные в ходе работы данные или действия с отдельными обьектами (файлами/папками) |

Модель «Деструктивное воздействие на СЗИ от НСД» (рис. 2.14) описывает действия злоумышленника по внедрению вредоносной программы посредством накопленных у него сведений о системе. Предварительный сценарий вредоносного воздействия злоумышленника на защищенный информационный ресурс АС разработан на основе анализа угроз представленных в банке данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России.

Вывод данной модели осуществлён в вершину r24 «Инициализация прав пользователя на работу в системе и доступ к каталогу файлов», которая отображает работу пользователя с внешним носителем информации.

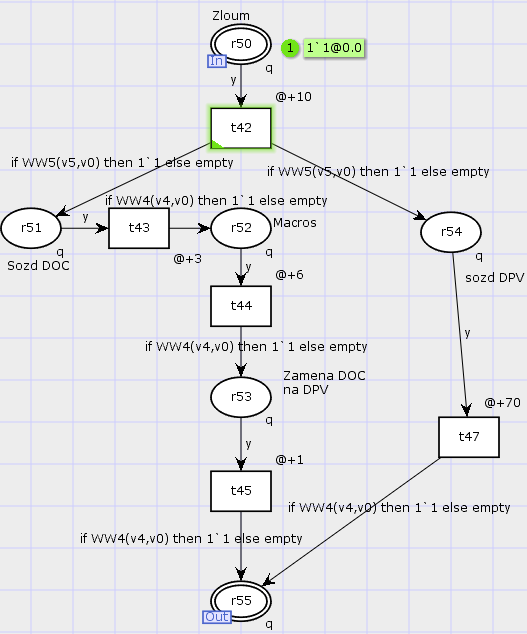


Рисунок 2.14. «Деструктивное воздействия на СЗИ от НСД»

Таблица 2.5. «Деструктивное воздействия на СЗИ от НСД»

|  |
| --- |
| Функции, выполняемые СЗИ от НСД |
| 5 Действия злоумышленника |
| 5.1 Создание документа |
| 5.2 Создание в документе вредоносной программы в виде макроса запускающийся вместе с документом |
| 5.3 Замена на носителе «чистого» документа вредоносным |
| 5.4 Создание Вредоносного ПО с функцией автозапуска |
| 5.5 Запись на носитель вредоносного документа или вредоносной программы |

Для успешного функционирования модели нужно объявить переменные и определить их значения. Чтобы это сделать нужно щелкнуть правой кнопкой мыши по элементу меню «Standard declarations» и выбрать пункт «New Decl», после чего в появившемся ниже поле нужно вписать нужные значения (рисунок 2.15). Оператор var служит для объявления переменной и для определения ее типа. Colset – для создания пространства цветов определенного типа. Val – для задания переменным определенных значений.

В CPN-Tools существует возможность подключения кода UML со стороннего файла, что позволит заметно сократить время обрабатывание модели и ускорить загрузку и обработку макета. Для того чтобы это реализовать нужно создать файл с расширением «.sml» и нужными функциями, однако это файл не должен содержать операнды объявления переменных и цветов, поскольку при подключении CPN-Tools к данному файлу будет логическая ошибка, так как программа «не знает» какие переменные использовать и посылать в те или иные функции. В нашем случае, данный файл выглядит так (рисунок 2.16), где Функции funWW. Реализованы для определения вероятностей переходов, например fun VV3(v02,v0)= (v02<=v0) отражает вероятность перехода 0.2. После создания файла нужно добавить декларацию (рисунок 2.17).

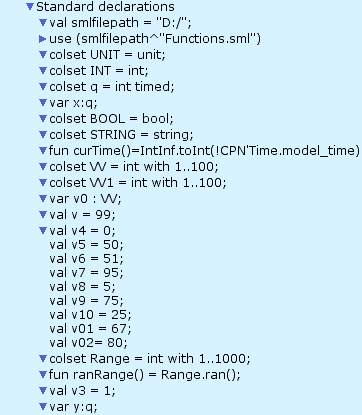


Рисунок 2.15. Фрагмент кода языка ML имитационной модели СЗИ от НСД

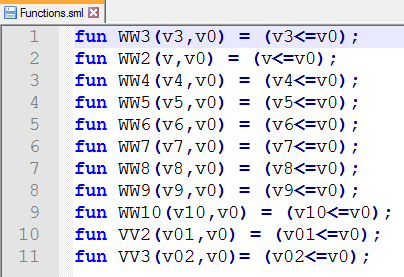


Рисунок 2.16. Файл .sml



Рисунок 2.17. Декларация в блоке CPN-Tools.

После всех проделанных операций получилась рабочая модель СЗИ от НСД. Это позволяет наглядно представить, что происходит при ее работе на системном уровне, а также учесть предполагаемые действия злоумышленника. Имитационная модель будет являться дискретной, динамической, стохастической по причине того, что этими свойствами обладает СЗИ от НСД в автоматизированной системе, поэтому данная модель будет дискретно-событийной, следственно, отражающей свойства во времени. Вероятность перехода из одного состояния в другое является мгновенной и зависит от времени пребывания в предыдущем состоянии.

**Глава 3. Сбор статистической информации**

## **3.1 Анализ полученной сети Петри**

Динамику функционирования механизмов защиты при определенных действиях пользователя в СЗИ от НСД в АС ОВД возможно описать при помощи маркировки сети Петри в результате срабатывания ее переходов. Представим данную динамику в виде графа разметок ориентированного графа , который показывает срабатывания каждого состояния исследуемой системы. Переходы  в данном графе представим в виде дуг. Разметку представим в виде последовательности цифр, описывающих положение маркеров в позиции при срабатывании того или иного перехода, – количество маркеров, а индексы используются для компактного представления, как, например, при  для графа . Начальная разметка графа представлена на рисунке 3.1.

В позиции  возможно накопление неограниченного количества маркеров, так как она имитирует собой журнал регистрации событий в СЗИ от НСД. Соответственно, при повторном прохождении по графу разметка графа  в позиции  будет с символом ** – это количество маркеров, которое характеризует объем записей в журнале событий СЗИ от НСД. Журнал событий является настраиваемым, т.е. администратор может установить объем, при котором он автоматически сохраняется на АРМ с дальнейшей возможностью его очистки.

Условия запуска перехода  сети Петри:.

Запуск перехода сети Петри: ,.

Граф разметок на рисунке 3.1 будет являться конечным, потому что действия пользователя с АС завершатся, по окончанию рабочего дня.

Проведем анализ основных свойств сети Петри представленной на рисунке и рисунке 3.1:

* неограниченность;
* безопасность;
* сохраняемость;
* активность;
* достижимость;
* покрываемость;
* эквивалентность.

Чтобы сделать конкретные выводы по работе защитных механизмов типовой СЗИ от НСД, охарактеризуем полученную сеть Петри.

Граф сети Петри является:

* неограниченным, так как количество фишек при проходе по графу изменчиво, т.е. не является постоянной величиной;
* небезопасным, так как число фишек в каждой позиции может превышать 1;
* несохраняемым, так как число циркулирующих объектов непостоянно, и число входов в отдельные переходы является большим, чем число выходов из него. Например, переход ;
* активным, что характеризуется тем, что данная сеть Петри не является тупиковой, так как может сработать каждый из переходов , где  – новая разметка графа. Сеть Петри по уровню активности является четвертой, так как найдется такая последовательность запусков переходов, что  будет разрешен;
* покрываемым, так как какую бы мы ни взяли разметку графа , она будет равна любой другой разметке .Пример: разметка  будет покрываема, так как ;
* достижимым, так как результатом запуска перехода в начальной разметке , является новая разметка , тогда разметка  является достижимой из . Маркировка  достижима, если существует последовательность запусков переходов  из . На рисунке 3.1 видно, что из начальной разметки можно пройти несколькими путями и получить конечную разметку;

Рисунок 3.1 – Граф разметок сети Петри типовой СЗИ от НСД в АС ОВД

* эквивалентным, что характеризуется возможностью оптимизации графа для удешевления процесса разработки, для распараллеливания конкретных функций с целью ускорения работы системы.

Модификация системы на практике осуществляется при помощи увеличения числа защитных механизмов для противостояния современным угрозам НСД, а сама структура (скелет) типовой СЗИ апробирована десятилетиями в различных сферах деятельности. В тоже время вопрос оптимизации остается открытым для других исследований с точки зрения нахождения наилучших взаимосвязей между функциональными компонентами СЗИ от НСД.

На основе выявленных свойств графа, выделим ключевые особенности моделируемой СЗИ от НСД:

* динамика функционирования исследуемой системы определяется неограниченностью, небезопасностью и несохраняемостью графа сети Петри. Можно сказать, что это обосновывается распараллеливанием процессов защитных механизмов и учетом несанкционированных действий в буфере программы. При проектировании подобных систем немаловажным фактором является оперативность реагирования на НСД;
* на рисунке 3.1 видно, что все переходы могут сработать, и в соответствии с этим можно сделать вывод, что структурно-логические связи механизмов защиты построены корректно;
* логику причинно-следственных связей отследим, основываясь на рисунке 3.1. Видно, что каждый компонент при определенных условиях может функционировать, взаимосвязи между ними корректны.

## **3.2 Обоснование количества проходов по имитационной модели для получения адекватных характеристик модели системы защиты информации от несанкционированного доступа**

Проверим полученную сеть на адекватность. В качестве примера продемонстрируем это на модели первой подсистемы. Для этогосделаем необходимое количество шагов, в результате которых, суммарное количество фишек в состояниях «r2» и «r4», «r04» и «r6», «r5» и «r7» составит 50. В позициях «r04» и «r6» 44 и 6 фишек рисунок 3.2, в позициях «r5» и «r7» 49 и 1 фишек рисунок 3.3. Тогда частоту появления фишек в состоянии «r2», «r6», «r7» рисунок 3.4 определим как:

|  |  |
| --- | --- |
|  | (1) |

Определим необходимое количество прогонов по сети для вероятности появления события с точностью  и достаточностью  по формуле.

|  |  |
| --- | --- |
| , | (2) |

где – функция Лапласа. Соответственно необходимое количество прогонов «r2», «r6», «r7», для данных состояний будет следующим:

|  |  |
| --- | --- |
|  | (3) |

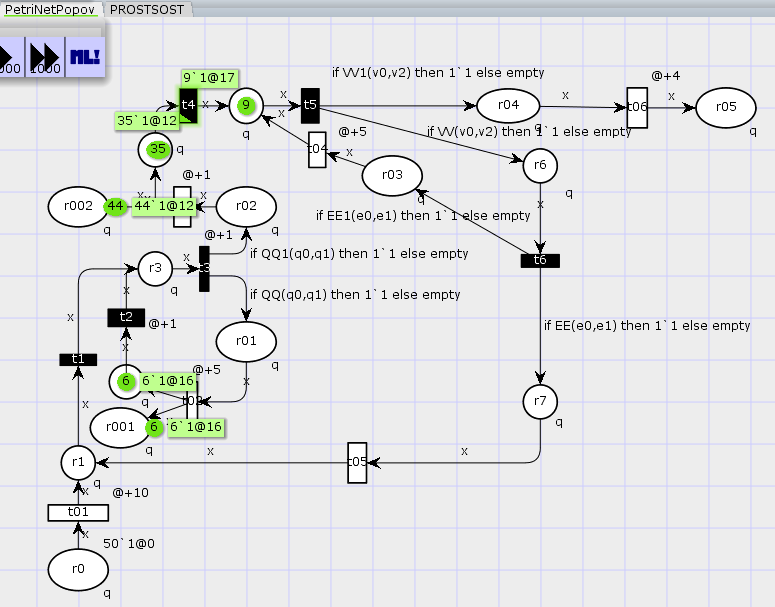


Рисунок 3.2 – Прогон модели для определения количества фишек в состояниях «r2» и «r4»

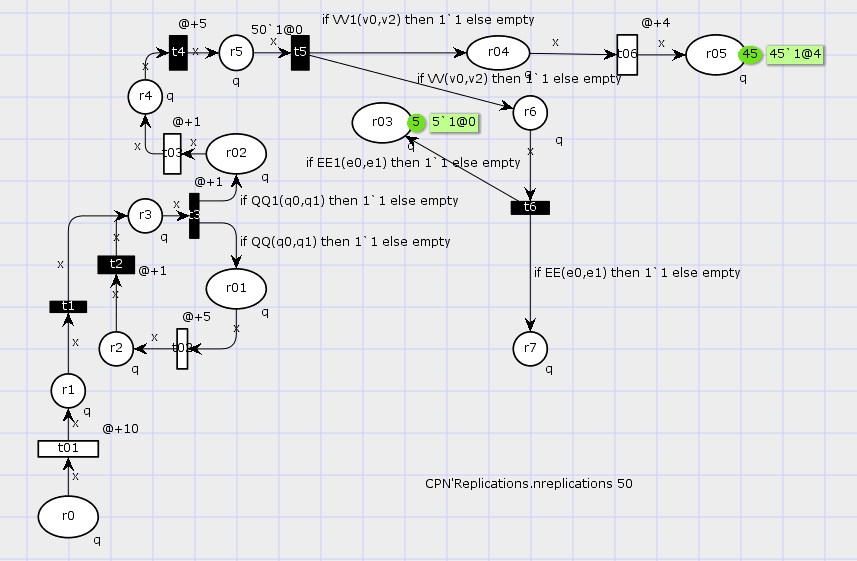
****

Рисунок 3.3 – Прогон модели для определения количества фишек в состояниях «r04» и «r6»

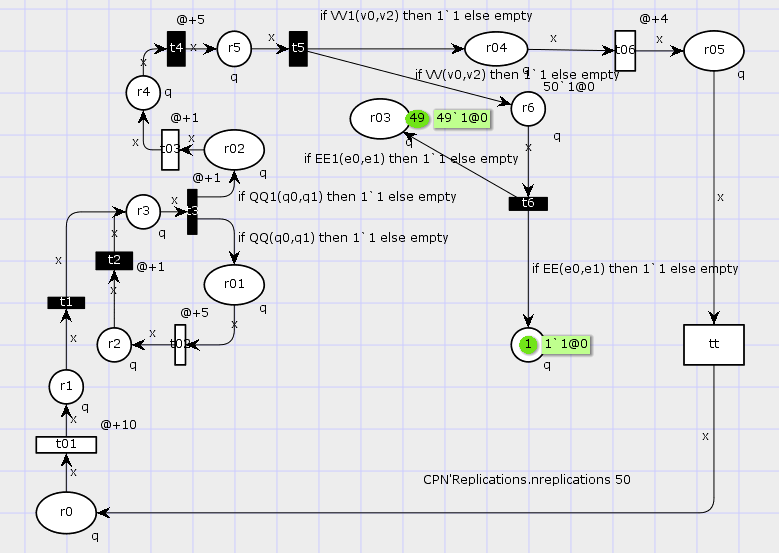
****

Рисунок 3.4 – Прогон модели для определения количества фишек в состояниях «r5» и «r7»

Выбираем наибольшее значение из трех и округляем его в большую сторону, тогда для подсистемы СЗИ от НСД «Вход в систему», необходимым количеством прогонов по сети составит . Рисунок 3.5.

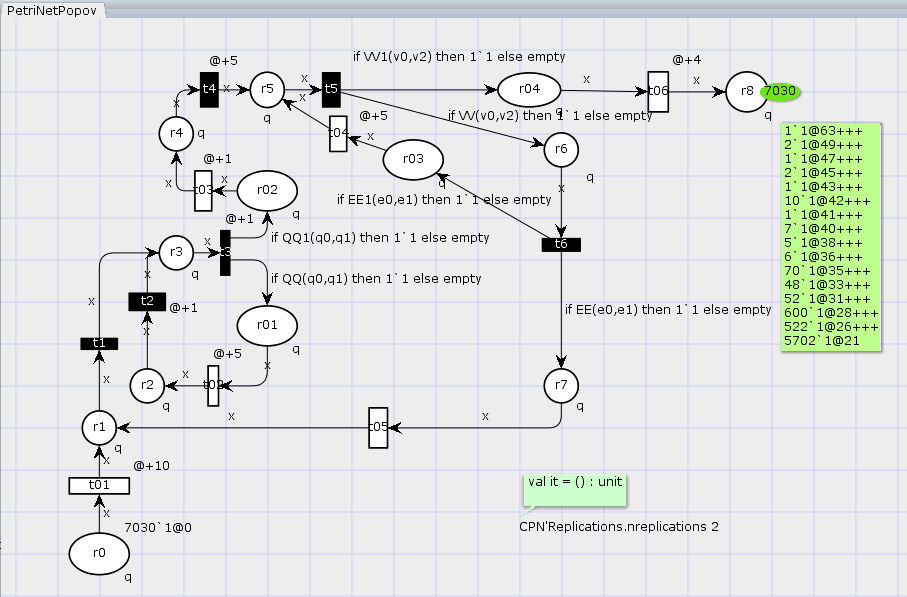
****

Рисунок 3.5 – Имитационная модель подсистемы «Вход в систему» СЗИ от НСД с необходимым количеством прогонов

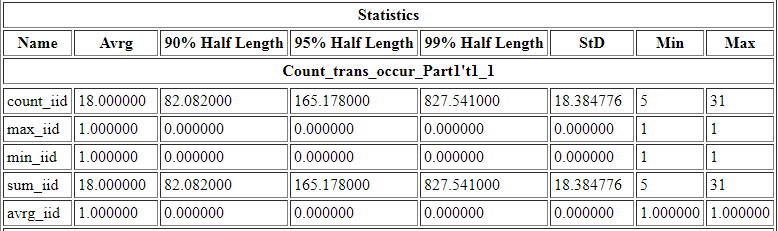
Согласно вышеприведенному примеру проделаем это для других подсистем и сведем результаты в таблицу 3.1. Необходимым количеством прогонов для всей имитационной модели составит *N*=16535.

Таблица 6. Сводная таблица расчетов необходимого количества прогонов имитационной модели СЗИ от НСД

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Начальная вершина | Конечная вершина | Кол-во фишек | Частота появления | N |
| Подсистема «Включение ПК и идентификации пользователя» | | | | |
| r3 | r2 | 6 | 0.12 | 7029.1584 |
| r3 | r4 | 44 | 0.88 | 7029.1584 |
| r5 | r6 | 5 | 0.1 | 5990.76 |
| r5 | r8 | 45 | 0.9 | 5990.76 |
| r6 | r7 | 1 | 0.02 | 1304.6544 |
| r6 | r5 | 49 | 0.98 | 1304.6544 |
| Подсистема «Инициализация прав пользователя на работу в системе и доступ к каталогу файлов» | | | | |
| r18 | r21 | 24 | 0.48 | 16614.3744 |
| r18 | r24 | 26 | 0.52 | 16614.3744 |
| r21 | r22 | 49 | 0.98 | 1304.6544 |
| r21 | r23 | 1 | 0.02 | 1304.6544 |
| r22 | r23 | 2 | 0.04 | 2556.0576 |
| r22 | r26 | 48 | 0.96 | 2556.0576 |
| r25 | r26 | 47 | 0.94 | 3754.2096 |
| r25 | r27 | 3 | 0.06 | 3754.2096 |
| r27 | r28 | 23 | 0.46 | 16534.4976 |
| r27 | r29 | 27 | 0.54 | 16534.4976 |
| Подсистема «Работа пользователя с файлами и программами» | | | | |
| r29 | r31 | 47 | 0.94 | 3754.2096 |
| r29 | r35 | 3 | 0.06 | 3754.2096 |
| r35 | r36 | 48 | 0.96 | 2556.0576 |
| r35 | r37 | 2 | 0.04 | 2556.0576 |
| r36 | r33 | 36 | 0.72 | 13419.3024 |
| r36 | r39 | 14 | 0.28 | 13419.3024 |
| r31 | r32 | 46 | 0.92 | 4899.1104 |
| r31 | r34 | 4 | 0.08 | 4899.1104 |
| Подсистема «Работа пользователя с прикладными программными продуктами» | | | | |
| r40 | r41 | 15 | 0.3 | 13978.44 |
| r40 | r42 | 17 | 0.34 | 14936.9616 |
| r40 | r43 | 18 | 0.36 | 15336.3456 |
| r42 | r45 | 6 | 0.12 | 7029.1584 |
| r42 | r46 | 8 | 0.16 | 8946,2016 |
| r42 | r47 | 10 | 0.2 | 10650,24 |
| r42 | r48 | 14 | 0.28 | 13419,3024 |
| r42 | r49 | 12 | 0.24 | 12141,2736 |
| Подсистема «Деструктивного воздействия на СЗИ от НСД» | | | | |
| r42 | r51 | 26 | 0.52 | 16614,3744 |
| r42 | r54 | 24 | 0.48 | 16614,3744 |

3.2. Получение статистической информации по имитационной модели

Для сбора статистических данных (мониторинга работы модели) используется палитра «Monitoring». После выполнения модели создастся файл с расширением .html который содержит элементы статистики. Для получения значений исследуемых характеристик после нескольких прогонов модели (например, 50) введем текстовое поле 17 «CPN’Replications.nreplications 50», кликнув правой клавишей мышки в пустом месте страницы и выбрав команду «Create aux text». Запустим модель, кликнув правой клавишей мышки по введенной надписи и выбрав соответствующую команду. В результате получим значения изучаемых характеристик после необходимого количества прогонов модели (рисунок 3.6).



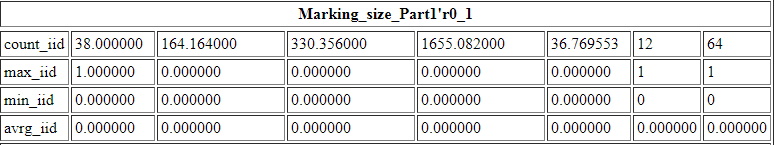


Рисунок 3.6. Статистические данные модели

Полный отчет об оценке мониторов имитационной модели СЗИ от НСД, связанных с пакетами для отправки очереди, очередью сетевого буфера и задержки пакетов данных. В столбце «Avrg» задается среднее значение оценок, собранных по совокупности симуляций. Столбец «95%» задает соответствующий доверительный интервал для каждой оценки, указывая значение, которое необходимо вычесть или прибавить к среднему, чтобы получить левую или правую конечную точку доверительного интервала. Столбцы «90%» и «99%» определяют доверительные интервалы аналогично «95%». В столбце «StD» указаны стандартные отклонения собранных оценок. Столбцы «Min» и «Max» соответственно представляют минимальные и максимальные значения собранных оценок.

На рисунке 3.7 приведена выдержка из отчета о доверительном интервале confidenceintervals95.txt. Первый столбец указывает сборщик данных и статистику, для которой был рассчитан доверительный интервал. Во втором столбце указан уровень доверительного интервала, т. е. 90, 95 или 99. В третьем столбце указано количество значений данных, для которых были рассчитаны среднее значение и доверительный интервал. Четвертый столбец - это длина половины доверительного интервала. Последние два столбца - это нижняя и верхняя конечные точки для доверительного интервала, т.е. [avrg-half length, avrg + half length].

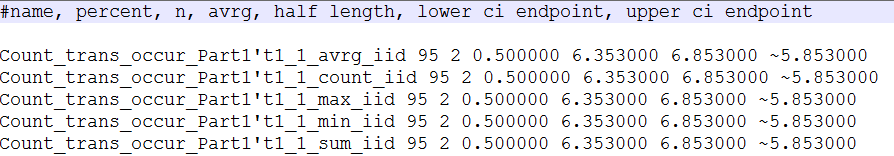


Рисунок 3.7. Отчет о доверительном интервале confidenceintervals95.txt.

Отчеты о производительности репликации содержат статистику, рассчитанную для значений данных, найденных в файлах журнала репликации. Поскольку весьма вероятно, что значения в файлах журналов репликации являются IID, доверительные интервалы в отчетах о производительности репликации с большей вероятностью будут точными, чем в отчетах о производительности моделирования.

## **3.3 Анализ пространства состояний**

При моделировании различных процессов возникает необходимость накопления и сохранения статистической информации о процессе моделирования (информация о маркировке, о срабатывании переходов, о созданных метках и другая). Для решения этой задачи в программе CPN Tools предусмотрены специальные инструменты мониторинга выполнения сети (мониторы).

Для использования данных инструментов необходимо открыть панель в области меню «Tool box → Monitoring», кликнув на ней левой кнопкой мыши и переместив в рабочую область. С помощью панели Monitoring (рисунок 3.7) переходам и позициям сети могут быть назначены различные мониторы, с помощью которых может быть зафиксировано изменение различных характеристик во время выполнения. Для назначения мониторов позициям и переходам необходимо присвоить им уникальные имена, при этом не допускается наличие пустых имен.

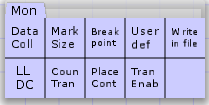


Рисунок 3.7. Панель Monitoring.

Для добавления монитора к элементу сети необходимо кликнуть левой кнопкой мыши на названии монитора, а затем на позиции или переходе, которому следует назначить данный монитор. После добавления монитора к элементу сети будет добавлена соответствующая запись в области меню (рисунок 3.8).

Для построения пространства состояний необходимо провести ряд проходов по имитационной модели, их количество обусловлено тем, чтобы маркер попал в каждую позицию, для построения всех возможных взаимосвязей. Пространство состояний рассчитывается полностью автоматически, с помощью инструмента «State Space», которая входит в палитру инструментов CPN Tools с использованием алгоритма расчета сетей Петри. Построение пространства состояний продолжается до тех пор, пока не останется больше вершин, однако в замкнутых сетях построение будет почти бесконечным. Как правило, за генерацией пространства состояний следует генерация strongly connected components (SCC) для определения поведения модели. Граф SCC группирует узлы, которые являются взаимно достижимыми, из этого следует, что он является ациклическим графом. Цикл, содержащий два SCC S и S, будет означает, что любой узел пространства состояний n в SCC S может быть достигнут из любого узла пространства состояний n в SCC S (и наоборот), и, следовательно, n и n будут в том же SCC, так как SCC максимальны.

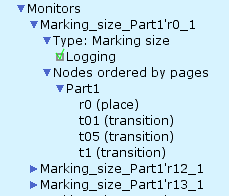


Рисунок 3.8. Запись в области меню о мониторах.

Каждая вершина графа пространства состояний имеет цифровые обозначения, верхнее означает номер шага по имитационной модели, левое нижнее обозначает количество входящих дуг, правое нижнее исходящих (рисунок 3.9). SCC-граф используется в CPN Tools, чтобы определить ряд стандартных поведенческих свойств модели и структуру SCC-графа что дает полезную информацию об общем поведении анализируемой модели.

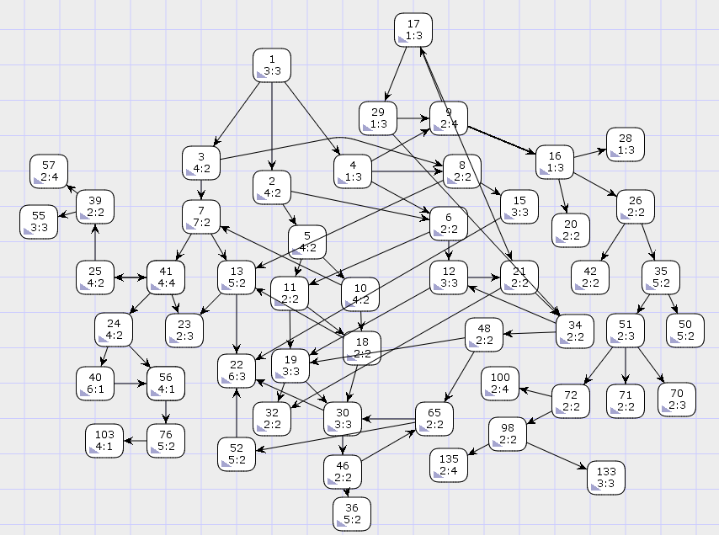


Рисунок 3.9. Пространство состояний имитационной модели СЗИ от НСД

С помощью пространства состояний можно наглядно увидеть взаимосвязи всей сети и зависимости вершин. После нажатия на треугольник в левом нижнем углу вершины можно увидеть полный список всех взаимосвязанных вершин и их состояния.

Элемент создания отчёта о пространстве состояний позволяет создать текстовый файл, в котором подробно описано состояние узлов и переходов, что позволяет вести статистику после каждого запуска модели.

Пространство состояний может быть очень большим, следовательно, его лучше анализировать его с помощью персонального компьютера (ПК). Первым шагом является построение отчёта о пространстве состояний, который предоставляет информацию о его размере, о поведенческих свойствах модели, а также о времени его построения, о количестве достижимых вершин и дуг. Отчет о пространстве состояний создается полностью автоматически и содержит информацию о ряде ключевых свойств анализируемой модели CPN. На рисунке 3.10 представлен отчет, в котором столбец Upper отражает максимальное количество маркеров в вершине, а столбец Lower минимальное. Что подтверждает логику построения модели т.к. один маркер моделирует действия пользователем, а другой злоумышленником.

Статистика (рисунок 3.11) отражает размер пространства состояний. Мы имеем 2196 вершин, 25182 дуг. Время на ее построение составило 2 сек. Мы также получили статистические данные о SCC-графе. Он имеет 51 достижимых вершин и 762 дуг, ведущих в эти вершины, и был рассчитан за 0 с. Тот факт, что вершин в SCC-графе меньше, чем в пространстве состояний говорит нам о том, что в пространстве состояний существуют циклы.

|  |  |
| --- | --- |
|  |  |
| Рисунок 3.10. Фрагмент отчета о количестве маркеров в имитационной модели | Рисунок 3.11. Фрагмент отчета о основной статистике. |

Также в отчете отражены свойства «домашней» вершины. Это такая вершина, в которую можно попасть от любой достижимой вершины, т.е. с любого узла в модели (рисунок 3.12).

Очередной элемент отчета – свойства живучести модели (рисунок 3.13). Существует некая «мертвая» вершина выхода из которой нет, следовательно, можно предположить, что модель построена правильно (если номер узла соответствует номеру конечной вершины в модели). Однако, так называемая «мертвая» вершина может являться «домашней».

|  |  |
| --- | --- |
|  |  |
| Рисунок 3.12. Свойства «домашней» вершины | Рисунок 3.13. Свойства живучести |

## **Вывод**

В данной дипломной работе разработана имитационная модель СЗИ от НСД. Проведен системный анализ ее функциональных компонентов который позволил выделить ее ключевые подсистемы. При помощи программного пакета CPN Tools в частности инструмента «Hierarchy» установлены взаимосвязи между подсистемами СЗИ от НСД. Установили взаимосвязи между компонентами СЗИ от НСД с использованием пространства состояний, что позволяет провести ее функциональный анализ. В работе были получены отчеты о работе имитационной модели, которые содержат в себе основную информацию о ее характеристиках. Обосновано количество прогонов системы для получения статистической информации

**СПИСОК ЛИТЕРАТУРЫ**

1. Разработка имитационной модели системы защиты информации от несанкционированного доступа с использованием программной среды CPN Tools / О. И. Бокова, Д. И. Коробкин, С. А. Кухарев, А. Д. Попов // Безопасность информационных технологий. – 2019. – №3(26). – С. 80 – 89.
2. СЗИ «Страж NT». Руководство администратора. URL: <http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf> (дата обращения: 23.09.2019).
3. Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. URL: <http://www.rubinteh.ru/public/opis30.pdf> (дата обращения: 23.09.2019).
4. Вентцель Е.С. Теория вероятностей. ‑ Москва. Наука, 1969, 576 с.
5. K. Jensen and L.M. Kristensen. [Colou](http://www.cs.au.dk/~cpnbook/)[red Petri Nets — Modeling and Validation of Concurrent Systems](http://www.cs.au.dk/~cpnbook/). Springer-Verlag Berlin, 2009.
6. Синегубов С.В. Моделирование систем и сетей телекоммуникаций. Воронеж: ВИ МВД РФ, 2016. - 336 с.
7. Zaitsev D.A., Shmeleva T.R. Simulating Telecommunication Systems with CPN Tools: Students' book. – Odessa: ONAT, 2006. – 60 p.
8. Григорьев В.А., Карпов А.В. Имитационная модель системы защиты информации : Международный журнал «Программные продукты и системы». – Тверь : МНИИПУ и НИИ «Центрпрограммсистем», 2005. – №2. – С. 26–30.
9. Питерсон Д.Ж. Теория сетей Петри и моделирование систем: Пер. с англ. ‑ М. : Мир, 1984. 264 с.
10. Котов В.Е. Сети Петри. ‑ М. : Наука. Главная редакция физико-математической литературы, 1984. 160 с.